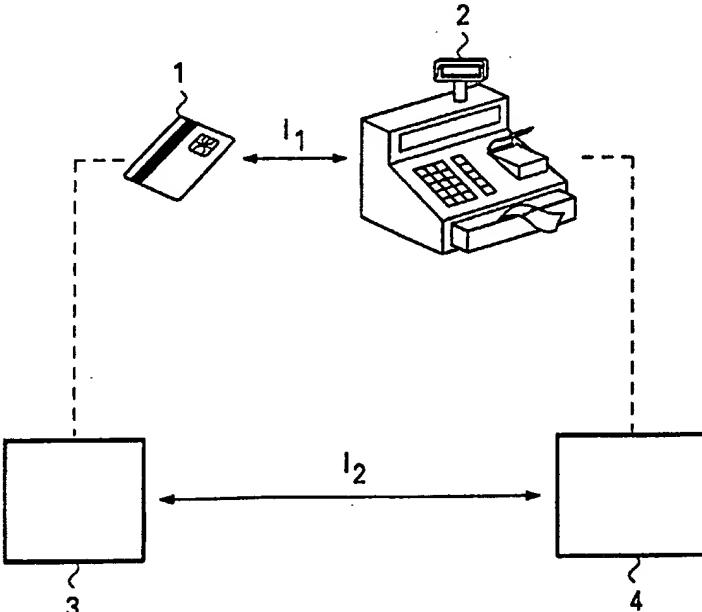


PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08, 19/00		A1	(11) International Publication Number: WO 96/36024 (43) International Publication Date: 14 November 1996 (14.11.96)
<p>(21) International Application Number: PCT/EP96/01938</p> <p>(22) International Filing Date: 8 May 1996 (08.05.96)</p> <p>(30) Priority Data: 1000352 12 May 1995 (12.05.95) NL</p> <p>(71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).</p> <p>(72) Inventors: DE ROOIJ, Peter, Jacobus, Nicolaas; Wijnpersstraat 30/13, B-3000 Leuven (BE). MULLER, Frank; Meerboet- laan 24, NL-2623 NJ Delft (NL). HIRSCHFELD, Rafael; Prinsengracht 748, NL-1017 LC Amsterdam (NL). BOLY, Jean-Paul; Loethe 22, NL-2381 BL Zoeterwoude (NL).</p>		<p>(81) Designated States: AU, BR, CA, CN, CZ, EE, HU, JP, KR, LT, LV, MX, NO, NZ, PL, SG, SI, SK, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>	
<p>(54) Title: ELECTRONIC PAYMENT SYSTEM HAVING SEVERAL CALCULATION UNITS, ELECTRONIC PAYMENT MEANS, AS WELL AS A METHOD FOR ELECTRONIC PAYMENT</p> <p>(57) Abstract</p> <p>The invention relates to a payment system with electronic payment means, such as electronic payment cards (1) such as "smart cards", and one or more payment stations (2), such as electronic cash registers. The payment stations are designed for receiving, during a payment transaction, a monetary value by crediting, in the payment station, a first value, and debiting, in the payment means, a second value corresponding to the first value. According to the invention, the first and second values may be expressed in different calculation units, such as currencies of different countries. The invention furthermore offers a payment means (1) for application in such a system, and a method for effecting a payment transaction with an electronic payment means.</p> 			

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

Electronic payment system having several calculation units, electronic payment means, as well as a method for electronic payment.

BACKGROUND OF THE INVENTION

The invention relates to a payment system having electronic payment means, such as so-called "chip cards" or "smart cards". More in particular, the invention relates to a payment system comprising electronic payment means

5 and one or more payment stations, which payment stations are designed for receiving, during a payment transaction, a monetary value by crediting, in the payment station, a first balance with a first value, and by debiting, in the payment means, a second balance with a second value corresponding to the first value, which balances represent numbers of calculation units.

10 Such payment systems, or generally systems for electronic payment having (electronic) payment means, are known in practice. Prior art payment means (payment cards) comprise one or more integrated circuits ("chips"), which are mounted on a plastic substrate. In such an arrangement, the at least one integrated circuit comprises a processing unit (microprocessor) for

15 carrying out, e.g., computations and cryptographic operations, and a storage unit (memory) for storing, e.g., monetary values and cryptographic data.

Monetary values may be recorded as counter readings, with a certain counter reading corresponding to a certain amount of money in the currency in question. In the event of application of such payment means in a payment

20 transaction, the monetary value is debited by lowering counter readings (possibly the contents of specific memory positions).

Since the possible applications of such payment means may be considerably extended if they are capable of being used in more than one country, it has been proposed to accommodate several currencies in one

payment means. For this purpose, the storage means are provided with several counters, each of which updates a value of a certain currency (valuta). At the same time, the payment means is designed to each time draw on that currency, which is used in the country in question. Thus, this prior art

5 payment means will have a counter which records a value in guilders (stock or "pot" of Dutch guilders) and another counter which records, e.g., a value in German marks. In this manner, it is possible in the Netherlands to pay with guilders and in Germany with marks.

Although a payment system having such prior art payment means is fit

10 for use, it has several drawbacks. Thus, the number of different currencies is limited by the number of counters on the card which, due to the available memory space (or capacity of the hardware) is bound by a maximum. If such a payment means has been in use for some time in a relatively large number of countries, many counters will be in use and in practice be occupied by a

15 small amount in foreign currency. This situation is similar to the one of ready cash, with a traveller, after his trip, in most cases being left with several coins of various currencies. As a result, it is not possible to add a new currency to the payment means without erasing a counter. In addition, such residual values together may constitute an expense for the user.

20 Prior art devices dealing with multiple currencies do not solve these problems. European patent application EP 0 251 619, for example, discloses a transaction card capable of performing payments in alternate currencies. A transaction limit may be converted into another currency, but the actual payments are made in a single currency, thus leaving the card holder with

25 unspent amount in various currencies.

International patent application WO93/08545 discloses a value transfer system having a plurality of electronic purses. Different currencies may be

loaded in the purses, and an amount held in a purse may be converted to a different currency. However, this conversion involves the floats of the respective currencies and cannot be handled by the card alone. This prior art payment system is thus not completely flexible with respect to different currencies.

5

SUMMARY OF THE INVENTION

The object of the invention is to eliminate the above and other drawbacks of the prior art and to provide a payment system which enables 10 currencies to be exchanged during a financing transaction, such as a payment transaction.

Another object of the present invention is to provide a payment system which allows an off-line conversion of currencies.

A further object of the invention is to provide a payment means for 15 application in such a payment system, as well as a method for safely processing payments in a payment system.

These and other objects are achieved with a payment system of the type referred to in the preamble, which for this purpose and according to the invention is characterised in that the payment means is arranged for 20 converting calculation units in such a manner that the first and second values may be expressed in different calculation units.

Because a conversion of calculation units has been provided, e.g. 25 currencies, may be converted. As a result, the first balance may be credited in a first currency (e.g., Dutch guilders), with the second balance being debited in a second currency (e.g., German marks).

Preferably, the payment system of the invention is implemented in such a manner that the second value is composed of at least a third and a

fourth value, each of which is expressed in a different calculation unit. In other words, the debiting of the second value may take place in more than one calculation unit. Thus, a payment may be effected by debiting the balance of several calculation units, such as by debiting two currencies (e.g., Dutch 5 guilders and German marks, or Dutch guilders and British pounds). This has the advantage that the holder of the card may dispose of several balances of the payment means, irrespective of the calculation unit in which the payment itself (i.e., the crediting of the first value) must take place. In addition, it is made possible in this manner to use up remaining balances, even if no 10 payments in the calculation units in question themselves are required.

Generally the first and second values, if they are expressed in the same currency, will be identical. It is conceivable, however, that e.g. transaction costs are charged, as a result of which the amount debited in the payment means may exceed the amount credited in the payment station.

15 Since it is possible with the payment means according to the invention to exchange currencies during a transaction, it is possible, in the event of payment, to debit several counters. As a result, in the first place the option is created of paying even if no sufficient balance is available of the currency required for the payment. After all, other currencies may be drawn on. In the 20 second place, the option exists of releasing counters by completely using up a balance of any currency (counter reset) if the amount to be paid is at least equal to the counter reading in question. In this manner, counters may be used for new currencies. In the third place, the option arises of computing a total balance of the payment means in a simple manner. Since, according to 25 the invention, the total balance may be converted into any currency, the user knows what are the maximum spending options of the payment means. In the fourth place, a spending limit may be set (by the user), i.e., not only for each

currency separately but also for the payment means as a whole. This spending limit may apply both to each transaction and cumulatively, i.e., for all transaction together.

As referred to above, the invention provides for the payment means, in 5 the event of a payment transaction, being debited with another currency than the one with which the payment station (e.g., an electronic cash register) is credited.

The invention further provides a device for managing payment means, as well as a system for effecting financial transactions.

10

EXEMPLARY EMBODIMENTS

The invention will be explained in greater detail below by reference to the Figures.

Fig. 1 schematically shows a system for effecting financial transactions.

15 Fig. 2 schematically shows a table having calculation units according to the invention.

Fig. 3 schematically shows a method for effecting, with an electronic payment means, a payment transaction according to the invention.

20 Fig. 4 schematically shows a device for managing a payment means according to the invention.

The system shown in Fig. 1 comprises a payment means 1, a payment station 2, a first financial institution 3 and a second financial institution 4. Between the payment means 1, which may be a so-called "smart card", and the payment station 2, there takes place an interaction I₁, as part of a financial 25 transaction. This interaction I₁ comprises the exchange of data, e.g., relating to the identity of the payment station and of the payment means, and amounts to be paid and the corresponding calculation units. In the event of a

transaction, such as a payment, not only are the values in question recorded, but also the calculation units of such values. The payment station 2 may be an electronic cash register which is designed for electronic payment with payment means such as payment means 1. Between the first financial institution 3 and the second financial institution 4, an interaction I_2 takes place which comprises, inter alia, the exchange of data relating to payments effected (such as in the interaction I_1). The first and second financial institutions may coincide.

As mentioned earlier, problems may arise in financial transactions with a payment means 1 if the payment means disposes of several different calculation units. According to the invention, such problems may be solved by permitting, in the payment system, that in one transaction payment may be effected with several calculation units. For this purpose, a table is stored in the payment means 1 as shown in Fig. 2. This table comprises rows, each having an amount (A), a calculation unit (C), a conversion factor (R) and possibly a priority factor (P). Regarding the first calculation unit, it is e.g. recorded that the amount A1 is 317.50, the calculation unit C1 is the German mark, the conversion factor R1 (as compared to a reference calculation unit) is 1.10, and the priority P1 is 2. Apart from a currency, the calculation unit may be, e.g., a telephone pulse; the reference calculation unit may be the currency of the country of issue (e.g., Dutch guilder), but also another currency or unit, such as the ECU or the Japanese yen. In the event of a payment transaction, the balance of the calculation unit required by the payment station is preferably debited by default. As an alternative, the reference calculation unit may serve as default unit. The reference calculation unit as such may be assigned a priority (P) equal to 1.

The conversion factors R1, R2, ... , which in the event of a currency

are exchange rates, are primarily informative: they give the user information relating to the value of the various balances. When a payment is effected, advantageously use will be made of a conversion factor which is stored in the payment station and which is updated regularly, e.g., daily.

5 The diagram of Fig. 3 shows, by way of example, a possible embodiment of the method according to the invention. The payment means 1 (see Fig. 1) is schematically referred to by I, the payment station 2 by II.

In step 100, there takes place an activation of the payment means. In the subsequent step 101, the payment means transmits data, including the
10 balances (amounts) A1, A2, ... AN, to the payment station. In step 102, the payment station displays these balances, preferably multiplied by their respective conversion factors. The user may now choose, e.g., with the help of a keyboard available on the payment station, or by intervention of a device according to Fig. 4, which balance or which balances he/she will draw on for
15 the payment, in other words, in which calculation unit (currency, pulse) he will pay. It may be advantageous to provide for a default value, such as the calculation unit required by the payment station.

In step 103, the user chooses the balances to be used. In this connection, it is checked whether the amounts to be paid do not exceed a
20 spending limit per calculation unit and/or per transaction. If such is the case, a return is made to step 103. If the spending limits have not been exceeded, in step 104 the payment data PD is composed of the balances chosen and supplementary (identification) information. In step 105, a random number α is generated and, together with the payment data PD, transferred to the
25 payment means. This random number α serves to protect the procedure and prevents so-called "replay" by third parties.

In step 106 it is verified, in the payment means, whether the total

amount to be paid is available and, by means of a cryptographic function S and a (secret) key s, a value ρ is produced which will be applied to verify the procedure.

In step 107, the balances in question (A in Fig. 2), as well as the 5 available amounts, are lowered. Possibly, a flag may be set ("busy") to indicate that the procedure may not be interrupted at this stage. Subsequently, in step 108 the value ρ is transferred to the payment station. In step 109, the payment station checks the value ρ , e.g., by enciphering the payment dates and the value a with a public key π and a function T, which is the inverse of 10 S: $T_\pi = S_\sigma^{-1}$. If the outcome of this operation indeed produces ρ , in step 110 an acknowledgement ACK is sent to the payment means, whereupon the payment means in step 111 resets the flag ("busy") set earlier. This concludes the transaction.

The method described above according to the invention therefore offers 15 both a conversion of calculation units and a verification of the payment means.

The device ("wallet") 7 for managing a payment means 1, which is schematically shown in perspective in Fig. 4, comprises an opening 71 for receiving the payment means 1, a keyboard 72 and a display screen 73. 20 Internally, the device 7 may comprise a control, a memory, and a connector for contacting the contacts 11 of the payment means 1. The control may comprise a microprocessor which is also able to carry out cryptographic operations. The connector constitutes the mechanical and electrical coupling to the payment means 1 but, in the event of contactless payment cards, it may 25 be replaced by other suitable means for realising an (electromagnetic) coupling to the payment means 1. In addition, the device 7 may be provided with means for exchanging data with a payment station by means of optical,

electrical and/or acoustical signals.

According to the invention, the device 7 is provided with means for converting calculation units, such as currencies. The table of Fig. 2 may be advantageously made visible on the display screen 73. In this manner, the 5 user is able to check the balances (A1, A2, ... in Fig. 2). The device 7 may advantageously display a total balance of the balances A1, A2,

It will be understood by those skilled in the art that the invention is not limited to the embodiments shown, and that many modifications and additions are possible without departing from the scope of the invention.

10

REFERENCES

- [1] EP 0 567 610 & WO 93/08545 & US 5 440 634
- [2] EP 0 518 365
- [3] EP 0 546 584
- 15 [4] EP 0 251 619 & US 4 766 293.
- [5] EP 0 542 298

CLAIMS

1. Payment system comprising electronic payment means (1) and one or more payment stations (2), which payment stations are designed for receiving, during a payment transaction, a monetary value by crediting, in the payment station, a first balance with a first value, and debiting, in the payment means, a second balance with a second value corresponding to the first value, which balances represent numbers of calculation units, characterised in that the payment means (1) is arranged for converting calculation units in such a manner that the first and second values may be expressed in different calculation units.
- 10 2. Payment system according to claim 1, wherein the payment means (1) comprises calculation means for converting calculation units.
3. Payment system according to claim 1 or 2, wherein the payment means (1) is designed for storing conversion factors between the calculation units.
- 15 4. Payment system according to claim 3, wherein the second value is composed of a third and a fourth value, each of which is expressed in a different calculation unit.
5. Payment system according to claim 3 or 4, wherein the payment means (1) is designed for determining a total balance, expressed in one calculation unit, of calculation units stored in the payment means.
- 20 6. Payment system according to any of the preceding claims, designed for setting a spending limit of a payment means.
7. Payment system according to any of the preceding claims, designed for debiting the second value on the basis of conversion factors which are stored in the payment station.
- 25 8. Payment system according to claim 7, designed for periodically updating the conversion factors stored.

9. Payment system according to any of the preceding claims, wherein the calculation units comprise currencies of different countries, preferably the Euro, *inter alia*.
10. Financial transaction, carried out with the help of a payment system
5 according to any of the preceding claims.
11. Electronic payment means, comprising a substrate and at least one integrated circuit with processing means, storage means and input and output means, with the storage means being arranged for storing balances for several calculation units, characterised by the processing means being arranged for
10 converting, during a payment transaction, the currency of a balance to be paid.
12. Payment means according to claim 11, designed for debiting, during a payment transaction, several balances held in different currencies.
13. Payment means according to claim 11 or 12, designed for storing exchange rates of currencies.
14. Payment means according to claim 13, designed for determining the total balance of all balances.
15. Payment means according to claim 13 or 14, designed for storing a spending limit, and only effecting a transaction if the spending limit is not exceeded.
16. Device (7) for managing a payment means (1) according to any of the claims 11 up to and including 15, the device (7) comprising storage means, processing means, input means and transfer means, characterised by means (72) for entering exchange rates of currencies, and by the transfer means being arranged for transferring entered data to the payment means.
17. Device according to claim 16, provided with means for cryptographically protecting data.
18. Method for effecting a payment with an electronic payment means (1)

and a payment station (2), comprising the determination of the amount to be paid and the associated calculation unit, the determination, on the basis of conversion values stored in the payment means, of a collection of amounts against which the amount to be paid will be debited, and the transfer to the
5 payment station (2) of the amount to be paid in the required calculation unit.

19. Method according to claim 18, wherein the authenticity of the payment means (1) is verified with the help of a cryptographic operation on a random number generated by the payment station (2).

20. Method according to claim 19, wherein it is verified whether the
10 amount to be paid does not exceed a previously determined spending limit.

1 / 3

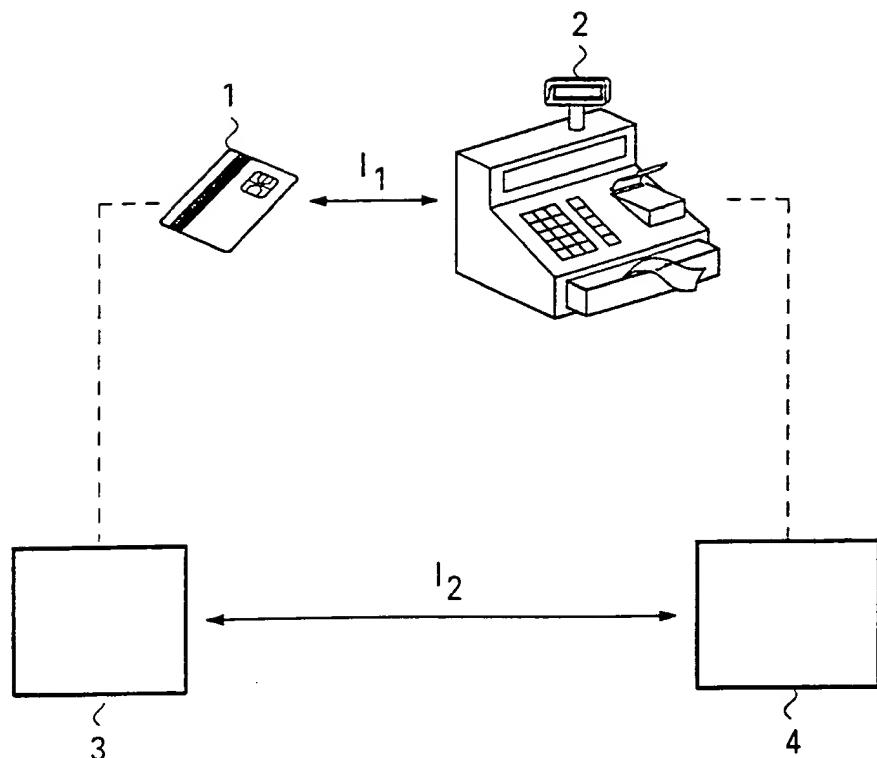


Fig. 1

A1	C1	R1	P1
A2	C2	R2	P2
A3	C3	R3	P3
...

Fig. 2

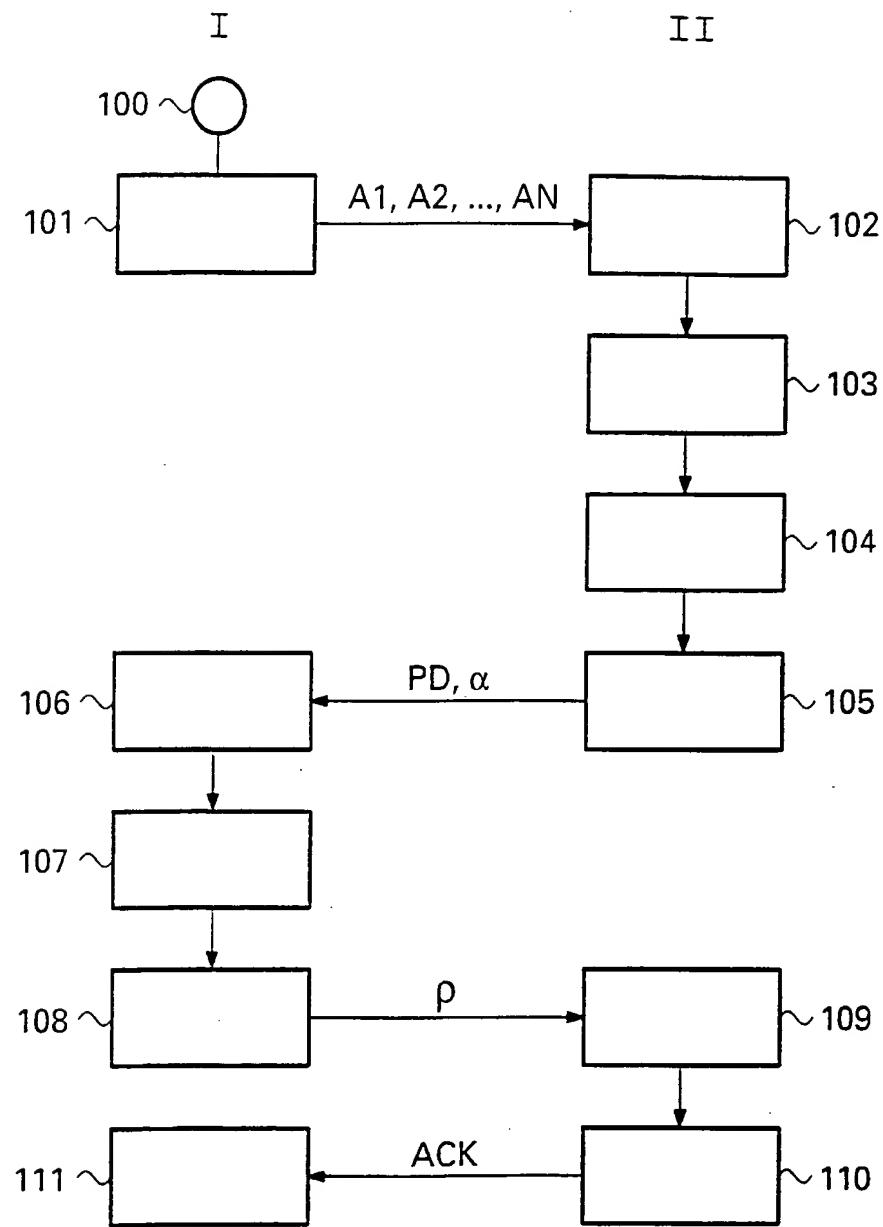


Fig. 3

3 / 3

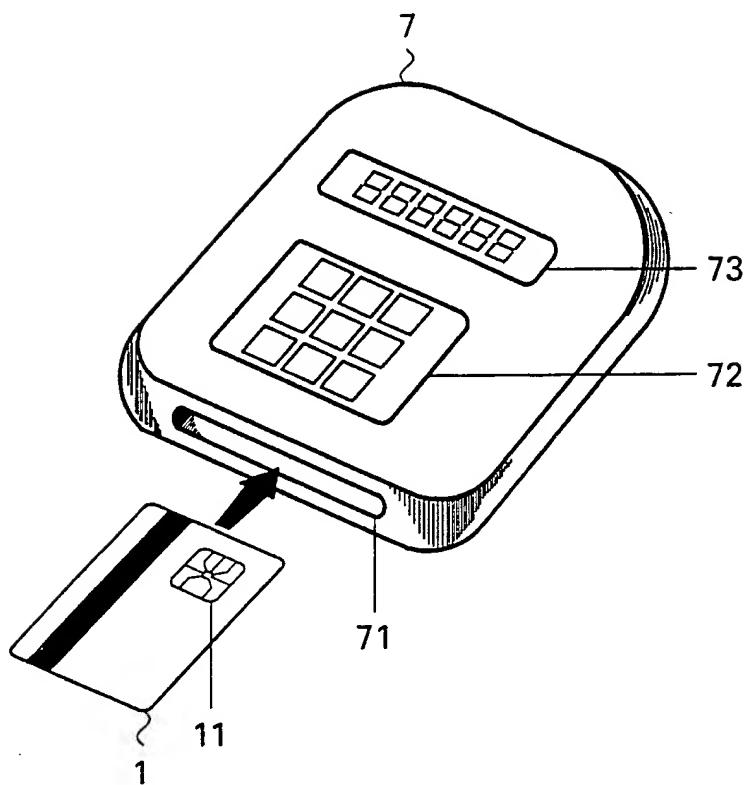


Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 96/01938

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F/08 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP,A,0 251 619 (VISA INTERNATIONAL SERVICE) 7 January 1988 cited in the application see abstract; claims; figures	1,10,18
A	see page 11, line 13 - page 17, line 11 ---	2-9,11, 13-17,20
Y	WO,A,93 08545 (JONHIG) 29 April 1993 cited in the application see abstract; claims; figures	1,10,18
A	see abstract; claims 1,2,27,33,39,49,58; figures 1-7,46-49 see page 35, line 37 - page 37, line 34 ---	5,6,15, 17,19,20
A	EP,A,0 542 298 (CITIBANK) 19 May 1993 see abstract; claims 1,2,27,33,39,49,58; figures 1-7,46-49 see page 35, line 37 - page 37, line 34 ---	1-3,5,6, 10,13, 15-20 -/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

&* document member of the same patent family

1

Date of the actual completion of the international search

Date of mailing of the international search report

21 August 1996

04.09.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

David, J

INTERNATIONAL SEARCH REPORT

International Application No

L1/EP 96/01938

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 234 954 (INTELLICARD INTERNATIONAL) 2 September 1987 ---	
A	EP,A,0 306 892 (J. DETHLOFF) 15 March 1989 -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
F.. /EP 96/01938

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0251619	07-01-88	US-A-	4766293	23-08-88
		AU-B-	587756	24-08-89
		AU-B-	7255987	07-01-88
		CA-A-	1270326	12-06-90
		DE-A-	3781606	15-10-92
		JP-B-	7089358	27-09-95
		JP-A-	63257089	24-10-88
WO-A-9308545	29-04-93	AU-B-	663739	19-10-95
		AU-B-	2888692	21-05-93
		BR-A-	9205416	17-05-94
		CA-A-	2098481	17-04-93
		EP-A-	0567610	03-11-93
		JP-T-	6503913	28-04-94
		PL-A-	299825	18-04-94
		US-A-	5440634	08-08-95
EP-A-0542298	19-05-93	US-A-	5453601	26-09-95
		AU-B-	2013695	20-07-95
		AU-B-	2013795	20-07-95
		AU-B-	2013895	20-07-95
		AU-B-	2013995	20-07-95
		AU-B-	658233	06-04-95
		AU-B-	2739292	17-06-93
		CA-A-	2080452	16-05-93
		CN-A-	1073789	30-06-93
		DE-T-	542298	16-12-93
		HU-A-	65212	02-05-94
		JP-A-	6162059	10-06-94
		JP-B-	7111723	29-11-95
		PL-A-	300041	05-04-94
		WO-A-	9310503	27-05-93
		US-A-	5455407	03-10-95
		ZA-A-	9208773	13-05-93
EP-A-0234954	02-09-87	WO-A-	8901207	09-02-89
EP-A-0306892	15-03-89	US-A-	4837422	06-06-89
		DE-A-	3867001	30-01-92
		JP-A-	1145798	07-06-89

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

P.. /EP 96/01938

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0306892	US-A-	4968873	06-11-90